2024/1101

12.4.2024

RECOMENDACIÓN (UE) 2024/1101 DE LA COMISIÓN

de 11 de abril de 2024

sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Vista la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 ([1]) (Directiva SRI 2),

Considerando lo siguiente:

(1) La protección de los datos y la seguridad de las comunicaciones sensibles son vitales para la sociedad, la economía, la seguridad y la prosperidad de la Unión. La ciberseguridad reviste una importancia estratégica para construir «Una Europa Adaptada a la Era Digital» ([2]) y constituye un objetivo clave del Programa Estratégico de la Década Digital ([3]).

(2) Tanto la Estrategia de la UE para una Unión de la Seguridad ([4]) como la Estrategia de Ciberseguridad de la UE ([5]) destacan el cifrado como una tecnología clave para garantizar la resiliencia, alcanzar la soberanía tecnológica y desarrollar la capacidad operativa a fin de prevenir los ciberataques. En efecto, el cifrado es esencial en el mundo digital para garantizar la seguridad de los sistemas y las transacciones digitales, proteger un conjunto de derechos fundamentales y garantizar las capacidades de defensa. La carrera emprendida por varios países y entidades privadas para desarrollar capacidades de computación cuántica y desbloquear nuevas oportunidades potencialmente provechosas plantea amenazas para las normas de cifrado actuales. Estas normas desempeñan un papel fundamental a la hora de garantizar la confidencialidad y la integridad de los datos, así como la protección de las comunicaciones sensibles, y prestar apoyo a elementos esenciales de la seguridad de las redes.

(3) El potencial de desarrollo en el futuro de ordenadores cuánticos capaces de descifrar los sistemas de cifrado actuales hace necesario que Europa busque salvaguardias más sólidas, garantizando la protección de las comunicaciones sensibles y la integridad a largo plazo de la información confidencial, es decir, debemos realizar la transición a la criptografía postcuántica lo antes posible. Este nuevo tipo de criptografía eliminará las vulnerabilidades conocidas de la actual criptografía asimétrica y mejorará la resistencia frente a las amenazas que plantea el uso malintencionado de los ordenadores cuánticos.

(4) La Comisión, consciente de la amenaza potencial que supone la computación cuántica para la actual criptografía de clave pública, lleva más de una década financiando la investigación y el desarrollo de la criptografía postcuántica.

(5) Los Estados miembros deben considerar la posibilidad de migrar sus actuales infraestructuras y servicios digitales para las administraciones públicas y otras infraestructuras críticas hacia la criptografía postcuántica lo antes posible, induciendo un cambio fundamental en los algoritmos, protocolos y sistemas criptográficos. Como se destaca en el reciente Libro Blanco de la Comisión titulado «¿Cómo abordar con éxito las necesidades de infraestructura digital de Europa?», lo anterior requiere un esfuerzo coordinado por parte de agencias gubernamentales, organismos de normalización, partes interesadas del sector, investigadores y profesionales de la ciberseguridad.

(6) La presente Recomendación de la Comisión anima a los Estados miembros a elaborar una estrategia global para la adopción de la criptografía postcuántica a fin de garantizar una transición coordinada y sincronizada entre los distintos Estados miembros y sus sectores públicos. La estrategia debe definir objetivos, hitos y plazos claros que den lugar a la definición de una hoja de ruta conjunta para llevar a cabo de manera coordinada la transición hacia

([1]) DO L 333 de 27.12.2022, p. 80.
([2]) COM(2020) 67 final.
([3]) Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030 (DO L 323 de 19.12.2022, p. 4).
([4]) COM(2020) 605 final.
([5]) JOIN(2020) 18 final.

una criptografía postcuántica. Estos pasos deberían conducir a la implantación, en toda la Unión, de tecnologías de criptografía postcuántica en los sistemas de administración pública y las infraestructuras críticas existentes a través de estrategias híbridas que podrían combinar la criptografía postcuántica con los enfoques criptográficos existentes o con la distribución cuántica de clave.

(7) Con objeto de facilitar una transición eficaz hacia la criptografía postcuántica, la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica debe proporcionar la lista de acciones que han de llevar a cabo los Estados miembros, incluido el examen de los algoritmos de criptografía postcuántica, con un calendario claro para las diferentes fases e hitos que deban alcanzarse, teniendo en cuenta sus interdependencias, así como las partes interesadas que deban participar.

(8) Para garantizar una aplicación armonizada de la criptografía postcuántica en toda la Unión, es esencial elaborar normas europeas comunes y un marco para identificar y seleccionar los algoritmos de criptografía postcuántica que vayan a implementarse en las redes y los servicios digitales en toda la Unión. A través de la participación activa de investigadores financiados por la UE, la Unión ya está apoyando, en el marco de procesos internacionales de selección en el ámbito de la criptografía postcuántica, el desarrollo y la prueba de algoritmos de criptografía postcuántica candidatos a convertirse en normas. La presente Recomendación de la Comisión anima a los Estados miembros a trabajar estrechamente a escala de la UE con los expertos en ciberseguridad de la Unión, con el Grupo de Cooperación SRI y con la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en la evaluación y selección de los algoritmos de criptografía postcuántica adecuados y su adopción como normas de la UE para una aplicación armonizada en toda la Unión.

(9) Los Estados miembros y la Unión deben seguir cooperando activamente con sus socios estratégicos internacionales en la elaboración de normas internacionales en el ámbito de la criptografía postcuántica, con vistas a garantizar la interoperabilidad de las comunicaciones en el futuro.

(10) Una vez acordada por los Estados miembros, la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica debe servir de modelo para la definición de los planes nacionales de transición hacia la criptografía postcuántica o, cuando existan planes nacionales, su adaptación a dicha hoja de ruta común.

(11) A fin de garantizar que se avanza en relación con los objetivos de la presente Recomendación, la Comisión tiene la intención de seguir de cerca las medidas adoptadas en respuesta a la misma. Por consiguiente, se anima a los Estados miembros a presentar a la Comisión, previa solicitud, toda la información pertinente que pueda esperarse razonablemente que faciliten para garantizar dicho seguimiento. Sobre la base de la información así obtenida y de cualquier otra información disponible, la Comisión evaluará los efectos de la presente Recomendación y determinará si son necesarias medidas adicionales, incluida la propuesta de actos vinculantes del Derecho de la Unión.

(12) La presente Recomendación sobre la criptografía postcuántica se basa en los objetivos establecidos en la Estrategia de Ciberseguridad de la UE con miras a la mejora de la seguridad de extremo a extremo y la resiliencia de las infraestructuras y servicios digitales de la Unión para las administraciones públicas y otras infraestructuras críticas; contribuye a los objetivos del mercado único digital y de la Comunicación conjunta sobre la Estrategia Europea de Seguridad Económica (10919/23) ([6]), y tiene en cuenta los riesgos para la seguridad física y cibernética de las infraestructuras críticas, así como los riesgos detectados en el marco de la evaluación de riesgos para las tecnologías cuánticas realizada recientemente ([7]). Respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la UE (artículos 7, 8 y 11) y el Convenio Europeo de Derechos Humanos (artículos 8 y 10), que implican obligaciones positivas para los Gobiernos de minimizar el riesgo de que se acceda a información y se obtenga su control de forma ilícita, lo que requiere la protección y promoción de las tecnologías criptográficas.

([6]) https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/es/pdf
([7]) JOIN(2023) 20 final.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN

1. ÁMBITO Y OBJETIVOS

El objetivo de la presente Recomendación es fomentar la transición hacia la criptografía postcuántica con objeto de proteger las infraestructuras y los servicios digitales para las administraciones públicas y otras infraestructuras críticas de la Unión, facilitando que los Estados miembros:

1) definan una «hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica» destinada a sincronizar sus esfuerzos para diseñar y aplicar planes nacionales de transición, garantizando al mismo tiempo la interoperabilidad transfronteriza;

2) apoyen la evaluación y selección de los algoritmos pertinentes de criptografía postcuántica de la UE con la ayuda de expertos en ciberseguridad y la posterior adopción de tales algoritmos como normas de la Unión que deben aplicarse en toda la Unión en el contexto de la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica;

3) adopten medidas adecuadas y proporcionadas a fin de prepararse para dicha transición.

2. HOJA DE RUTA PARA LLEVAR A CABO DE MANERA COORDINADA LA TRANSICIÓN HACIA UNA CRIPTOGRAFÍA POSTCUÁNTICA

4) La presente Recomendación anima a los Estados miembros a coordinar sus acciones a escala de la Unión a través de un foro específico de los Estados miembros. A tal fin, la Comisión recomienda que los Estados miembros aprovechen las estructuras existentes a escala de la Unión en el ámbito de la ciberseguridad y creen un subgrupo del Grupo de Cooperación SRI. Dicho subgrupo podría incluir a representantes de las agencias nacionales de seguridad y expertos en ciberseguridad, en particular de las autoridades nacionales de ciberseguridad y la ENISA. El subgrupo puede invitar a representantes de las partes interesadas pertinentes a participar en sus trabajos, como los de los órganos consultivos de las organizaciones públicas, la industria, los proveedores de servicios y los operadores, con vistas a recabar aportaciones e intercambiar información sobre la transición de las infraestructuras y servicios digitales para las administraciones públicas y otras infraestructuras críticas a la criptografía postcuántica en diferentes sectores, coordinar sus esfuerzos a escala nacional y elaborar la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica, de conformidad con las normas de competencia y la legislación en materia de protección de datos de la Unión.

5) Dicho subgrupo sobre criptografía postcuántica debe estudiar medidas adecuadas, eficaces y proporcionadas para definir y coordinar el desarrollo de la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica. Se anima al subgrupo sobre criptografía postcuántica a entablar debates con otros organismos pertinentes, como Europol, la OTAN u otros, a fin de evitar la duplicación de esfuerzos y garantizar un enfoque cohesivo para hacer frente a los retos emergentes.

6) A tal efecto, se invita a los Estados miembros a que, poco después de la publicación de la presente Recomendación, creen dicho subgrupo sobre criptografía postcuántica de conformidad con la Decisión de Ejecución (UE) 2017/179 de la Comisión ([8]) y designen a representantes expertos que trabajen en estrecha cooperación con la Comisión y a los que se encomienden la definición y el desarrollo de la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica.

7) Se debería disponer de la hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica en un período de dos años a partir de la publicación de la presente Recomendación. Una vez que se cuente con la hoja de ruta, cada Estado miembro elaborará y adaptará su propio plan de transición a la criptografía postcuántica, de conformidad con los principios establecidos en dicha hoja de ruta.

3. ACCIONES A ESCALA DE LA UNIÓN

8) La Comisión, en cooperación con los representantes expertos de los Estados miembros, realizará el seguimiento y la evaluación del conjunto de los trabajos.

([8]) Decisión de Ejecución (UE) 2017/179 de la Comisión, de 1 de febrero de 2017, por la que se establecen las disposiciones de procedimiento necesarias para el funcionamiento del Grupo de cooperación a que se refiere el artículo 11, apartado 5, de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 28 de 2.2.2017, p. 73).

9) A tal efecto, la Comisión podrá solicitar a los representantes de los Estados miembros que presenten toda la información pertinente que pueda esperarse razonablemente que faciliten a fin de garantizar el seguimiento de los avances logrados en la elaboración de dicha hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica y la eficacia de dichas medidas.

10) Sobre la base de esa y otra información disponible, la Comisión evaluará las medidas diseñadas y el funcionamiento de la red de representantes de los Estados miembros y determinará si son necesarias acciones adicionales, incluida la propuesta de actos vinculantes del Derecho de la Unión.

4. **REVISIÓN**

11) Los Estados miembros deben cooperar con la Comisión para evaluar los efectos de la presente Recomendación como máximo tres años después de su publicación, con vistas a determinar la forma adecuada de seguir avanzando. Esta evaluación debe tener en cuenta los resultados del trabajo del subgrupo de expertos nacionales sobre criptografía postcuántica.

Hecho en Bruselas, el 11 de abril de 2024.

Por la Comisión
Thierry BRETON
Miembro de la Comisión